WHAT IS CLAIMED IS:

1. A method for protecting digital television from unauthorized digital receivers within a population of digital receivers, where each digital receiver in the population has a unique identifier, the method comprising steps of:

receiving provisioning information from a subset of the population of digital receivers indicating that the subset is potentially within range to receive digital television from a broadcaster;

distributing first decryption information to the subset of the population of digital receivers, wherein:

the first decryption information allows for potentially decrypting a plurality of programs coextensively in time, and

the unauthorized digital receivers are cryptographically excluded from using the first decryption information;

encrypting first content using a first method that is cryptographically related to second decryption information;

sending the first content; and

distributing the second decryption information that is cryptographically secured with the first decryption information.

2. The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, further comprising steps of:

encrypting second content using a second method that is cryptographically related to third decryption information, wherein at least one of an algorithm, a key and a key length of the second method is different from that of the first method;

sending the second content; and

distributing third decryption information that is cryptographically secured with the first decryption information.

3. The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, further comprising a step of uniquely encrypting the first decryption information for each of the subset, wherein the first-

listed distributing step comprises sending first description information uniquely encrypted for each of the subset.

4. The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, further comprising a step of determining the unauthorized digital receivers to exclude from the subset of the population of digital receivers.

5. The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, wherein the first decryption information is uniquely encrypted for each of the subset.

6. The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, wherein the first decryption information comprises a key for decrypting the second decryption information.

7. The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, wherein the first decryption information expires by changing keys, key lengths and/or algorithms used to encrypt the first content.

8. The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, further comprising a step of forwarding the provisioning information to another broadcaster within range of one of the subset.

9. The method for protecting digital television from unauthorized digital receivers within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 1, wherein the unique identifier includes a key.

10. A computer-readable medium having computer-executable instructions for performing the computer-implementable method for protecting television from unauthorized digital receivers within the population of digital receivers of claim 1.

11. A computer system adapted to perform the computer-implementable method for protecting digital television from unauthorized digital receivers within the population of digital receivers of claim 1.

12. A method for processing digital television within a population of digital receivers, where each digital receiver in the population has a unique identifier, the method comprising steps of:

sending provisioning information from a subset of the population of digital receivers indicating that the subset is within range to receive digital television from a broadcaster;

receiving first decryption information with the subset of the population of digital receivers, wherein:

the first decryption information allows for potentially decrypting a plurality of programs coextensively in time, and

the unauthorized digital receivers are cryptographically excluded from using the first decryption information;

receiving first content;

receiving second decryption information that is cryptographically secured with the first decryption information; and

decrypting the first content using a first method that is cryptographically related to the second decryption information.

13. The method for processing digital television within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 12, further comprising steps of:

receiving second content;

receiving third decryption information that is cryptographically secured with the first decryption information; and

decrypting the second content using a second method that is cryptographically related to the third decryption information, wherein at least one of an algorithm, a key and a key length of the second method is different from that of the first method.

14. The method for processing digital television within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 12, wherein the first decryption information is uniquely encrypted for each of the subset.

15. The method for processing digital television within the population of digital receivers, where each digital receiver in the population has the unique identifier as recited in claim 12, wherein the unique identifier includes a key.

16. A computer-readable medium having computer-executable instructions for performing the computer-implementable method for processing digital television within the population of digital receivers of claim 12.

17. A computer system adapted to perform the computer-implementable method for processing digital television within the population of digital receivers of claim 12.

18. A method for protecting digital television from unauthorized digital receivers within a population of digital receivers, the method comprising steps of:

determining a first subset of the population of digital receivers, wherein the first subset is within range to receive digital television from a broadcaster;

distributing first decryption information to the first subset of the population of digital receivers, wherein:

the first decryption information is uniquely encrypted for each of the first subset, and

the first decryption information expires at some future time;

encrypting first content that is cryptographically protected from use by digital receivers without the first decryption information;

sending the first content in encrypted form;

determining the unauthorized digital receivers to exclude from the first subset to find a second subset of the population of digital receivers;

distributing second decryption information to the second subset of the population of digital receivers, wherein the second decryption information is uniquely encrypted for each of the second subset;

encrypting second content that is cryptographically protected from use by digital receivers without the second decryption information; and

sending the second content in encrypted form after the first decryption information has expired.

19. The method for protecting sending digital television from unauthorized digital receivers within the population of digital receivers as recited in claim 18, wherein the first and second decryption information assists in decrypting messages with keys that allow decrypting the first content.

20. A computer-readable medium having computer-executable instructions for performing the computer-implementable method for protecting digital television from unauthorized digital receivers within the population of digital receivers of claim 18.

21. A computer system adapted to perform the computer-implementable method for protecting digital television from unauthorized digital receivers within the population of digital receivers of claim 18.

22. A content receiver for protecting content that is transmitted with digital encoding, the content receiver comprising:

provisioning information that is sent away from the content receiver for a plurality of content broadcasters coupled to the content receiver;

first decryption information received from a point remote to the content receiver, wherein an unauthorized content receiver is excluded from using the first decryption information;

an interface coupled to content signals broadcast to a plurality of content receivers, wherein the content signals carry a plurality of programs coextensively in time;

second decryption information received from a place remote to the content receiver, wherein the second decryption information is cryptographically secured with the first decryption information; and

first content received with the interface, wherein the first content is decrypted with a method related to the second decryption information.

23. The content receiver for protecting content that is transmitted with digital encoding as recited in claim 22, wherein the content signals are protected by a plurality of encryption keys.

24. The content receiver for protecting content that is transmitted with digital encoding as recited in claim 23, wherein the first decryption information includes a category key.

25. The content receiver for protecting content that is transmitted with digital encoding as recited in claim 22, wherein the first decryption information includes a category key.

26. The content receiver for protecting content that is transmitted with digital encoding as recited in claim 22, wherein the second decryption information includes a content key.

27. The content receiver for protecting content that is transmitted with digital encoding as recited in claim 22, wherein the first decryption information expires after a period of time.

28. The content receiver for protecting content that is transmitted with digital encoding as recited in claim 27, wherein the period of time is two hours, one day, one week, one month, or one year.

29. The content receiver for protecting content that is transmitted with digital encoding as recited in claim 22, wherein the first decryption information is uniquely encrypted for each of a plurality of content receivers in a system.

30. The content receiver for protecting content that is transmitted with digital encoding as recited in claim 22, further comprising a plurality of content keys, wherein the first content is protected with one of the plurality of content keys.

31. The content receiver for protecting content that is transmitted with digital encoding as recited in claim 30, wherein the first decryption information includes a category key.